



IP-Netzwerke und Protokolle

- Überblick über die IEEE 802.x Richtlinien
- Grundsätzliches zu TCP/IP und UDP/IP
- Namen und Adressen (kurz)
- Gateways, Routing
- Praktische Übungen anhand der Linux-Standard-Tools



IEEE 802 Richtlinien (1)

- **802.1:** Higher Layer Interface Standard
- **802.2:** Logical Link Control
 - Typ 1: Datagramm-Dienste (verbindungslos)
 - Typ 2: Verbindungsorientierte Dienste
- **802.3:** CSMA/CD Zugriff (Ethernet)
- **802.4:** Token Bus Zugriffsverfahren
- **802.5:** Token Ring Zugriffsverfahren
- **802.6:** Metropolitan Area Network



IEEE 802 Richtlinien (2)

- **802.7:** Broadband Advisory Group
- **802.8:** Optical Fibre Technology Advisory Group
- **802.9:** Sprach/Daten-Integration in LANs
- **802.10:** Standard für LAN Security
- **802.11:** Wireless Standards
- **802.30:** 100BaseT, Standard für das CSMA/CD Ethernet mit 100 Mbit/s



Das Internet Protokoll Modell

- **Layer 4: Anwendungsschicht**
 - ISO/OSI Layer 7, 6, 5
- **Layer 3: Host-zu-Host-Transportschicht**
 - ISO/OSI Layer 4
- **Layer 2: Internetschicht**
 - ISO/OSI Layer 3
- **Layer 1: Netzzugangsschicht**
 - ISO/OSI Layer 2, 1

„Hierarchie“ der IP-Header

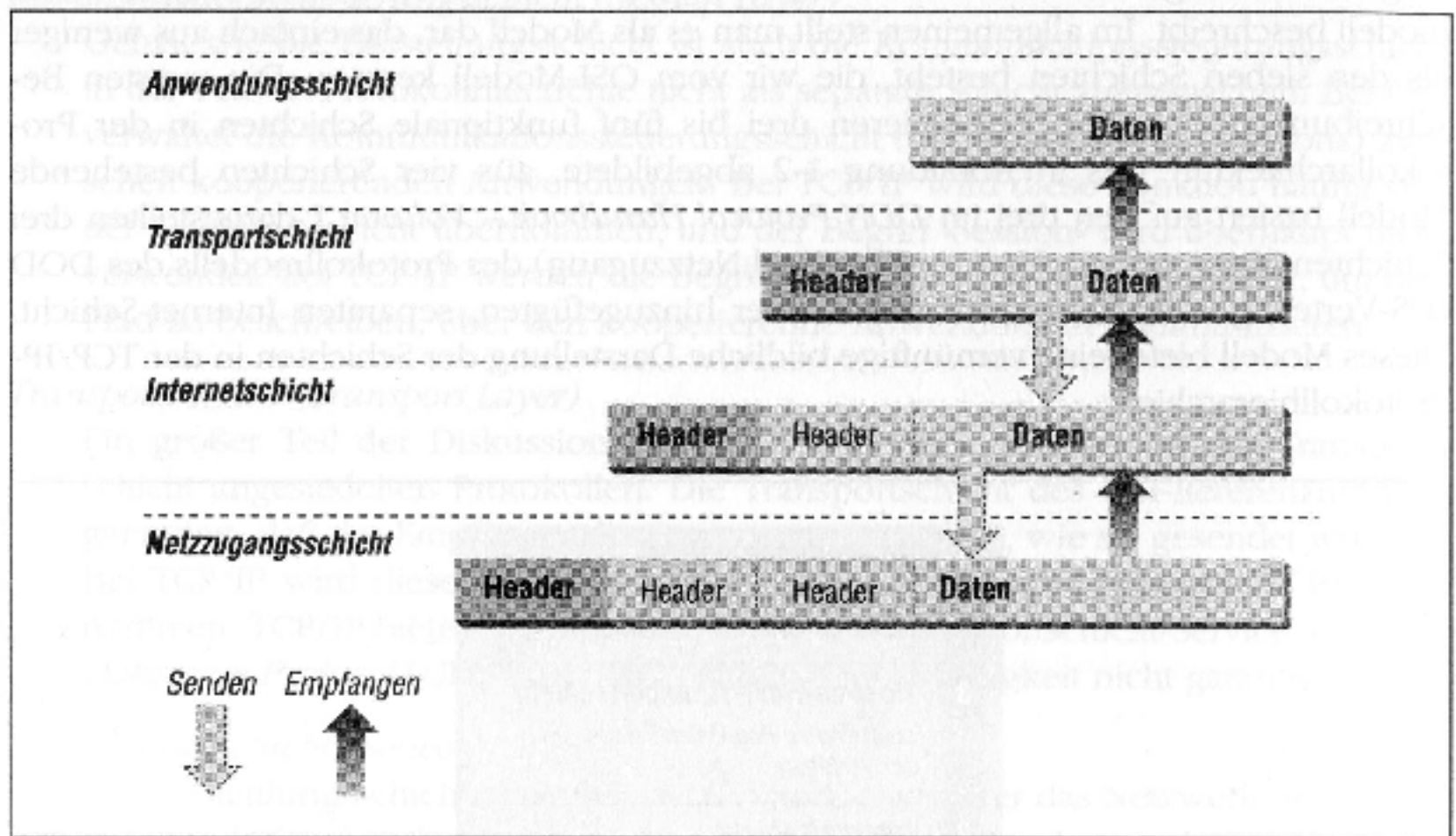


Abbildung 1-3: Die Kapselung von Daten



Netzzugangs-Schicht

- Weiß, wie die Hardware arbeitet,
- Kennt Details des realen Netzwerkes,
- Bietet eine abstrakte Schnittstelle zur nächst höheren (Internet-) Schicht,
- Dadurch muss in den höheren Schichten keine Rücksicht auf die „Physik“ des Netzwerkes genommen werden.
- RFC 826 (ARP), RFC 894 (Kapselung)

Address Resolution Protocol

- RFC 826 definiert, wie IP-Adressen in Hardware-Adressen abgebildet werden.
- Dazu werden Tabellen auf Hardware-Ebene benutzt, z.B. in Ethernet-HW und Routern.
- Jede Station hat eine MAC-Adresse, dargestellt als 6x2 Hex-Ziffern, z.B.

00-0D-88-9F-35-B9

- Reverse-ARP (RARP) setzt MAC-Adressen in IP-Adressen um.



Internet-Schicht

- Internet Protocol, RFC 791.
- Definition des **Datagramms** = Übertragungseinheit im Internet,
- Definition des Internet-**Adressierungsschemas**,
- **Datenübertragung** zwischen Netzzugangs- und Transportschicht,
- **Routing** von Datagrammen zu entfernten Hosts,
- **Fragmentierung** und **Defragmentierung** von Datagrammen.

Aufbau des IP-Headers

Version	IHL	Type of Service	Total Length	
Identification		Flags	Fragment Offset	
TTL	Protocol		Header Checksum	
Source Address				
Destination Address				
Options			Padding	
Data				

Abbildung 9.10: Format des IP-Headers



IP-Header: Wichtige Felder (1)

- Version: IP-Protokoll-Version
- IHL: Internet Header Length, Anzahl 32-Bit-Worte (siehe Padding!)
- Total Length: Gesamtlänge des Datagramms, max. 64 Kbyte
- Identification, Flags, Fragment Offset: Steuern die Fragmentierung / Re-Assembly
- Time to Live (TTL): „Hop Count“



IP-Header: Wichtige Felder (2)

- Protocol: Das ULP (upper layer protocol)
 - 1: ICMP: Internet Control Message Protocol
 - 3: GGP: Gateway-to-Gateway-Protocol
 - 6: TCP: Transmission Control Protocol
 - 8: EGP: External Gateway Protocol
 - 17: UDP: User Datagram Protocol
- Options: Routing-Vorschriften, Timestamps
- Padding: Füllbits, um den Header auf eine glatte Grösse zu bringen (32-Bit-Worte!)



Internet Control Messages (1)

- ICMP kennt folgende Nachrichtentypen:
- 0 Echo reply
- 3 Destination unreachable
- 4 Source quench
- 5 Redirect
- 8 Echo request
- 11 Time exceeded for datagram



Internet Control Messages (2)

- 12 Parameter problem on a datagram
- 13 Timestamp request
- 14 Timestamp reply
- 15 Information request
- 16 Information reply
- 17 Address mask request
- 18 Address mask reply

Routung über Gateways (1)

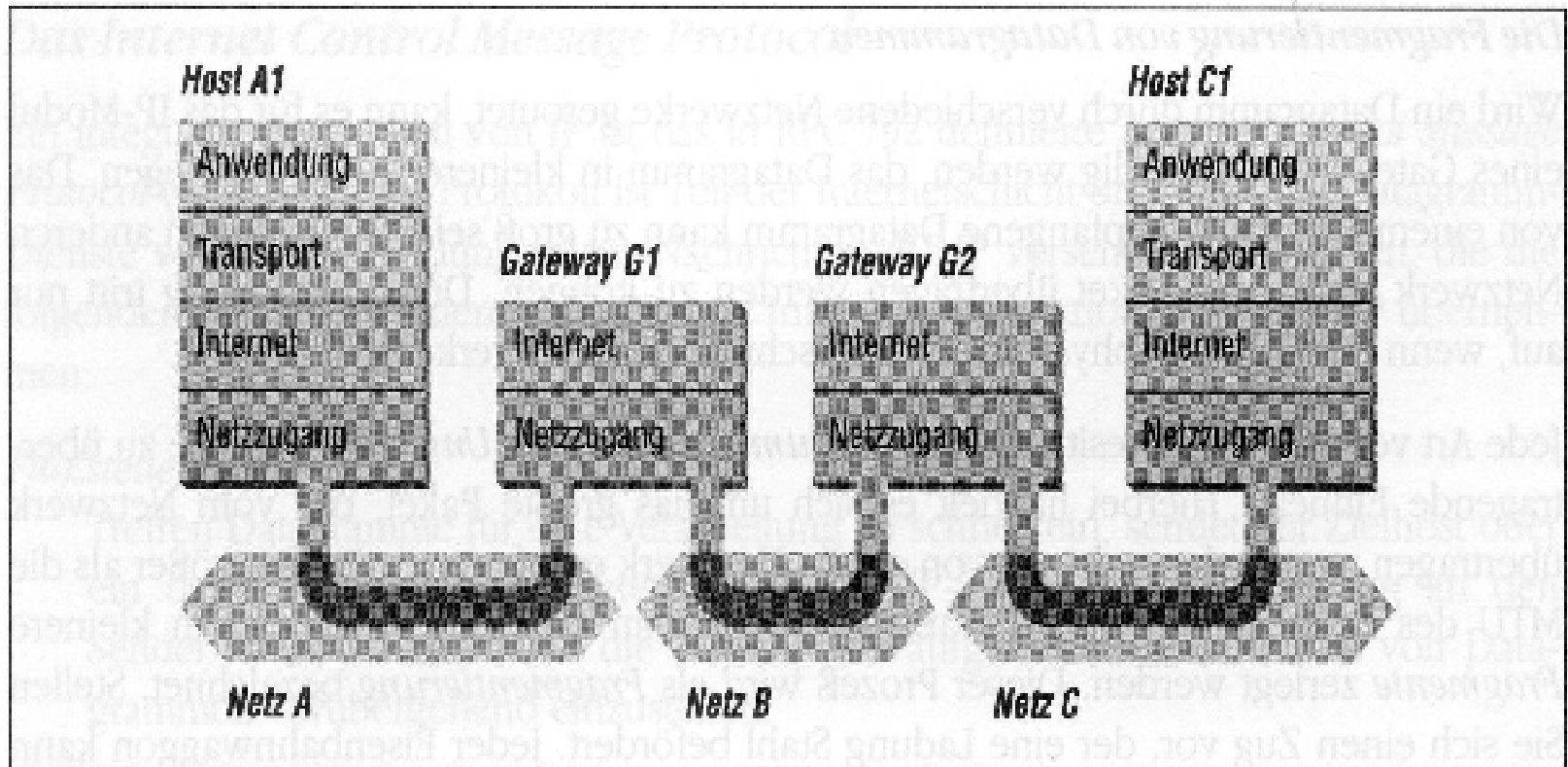


Abbildung 1-6: Routing über Gateways

Routung über Gateways (2)

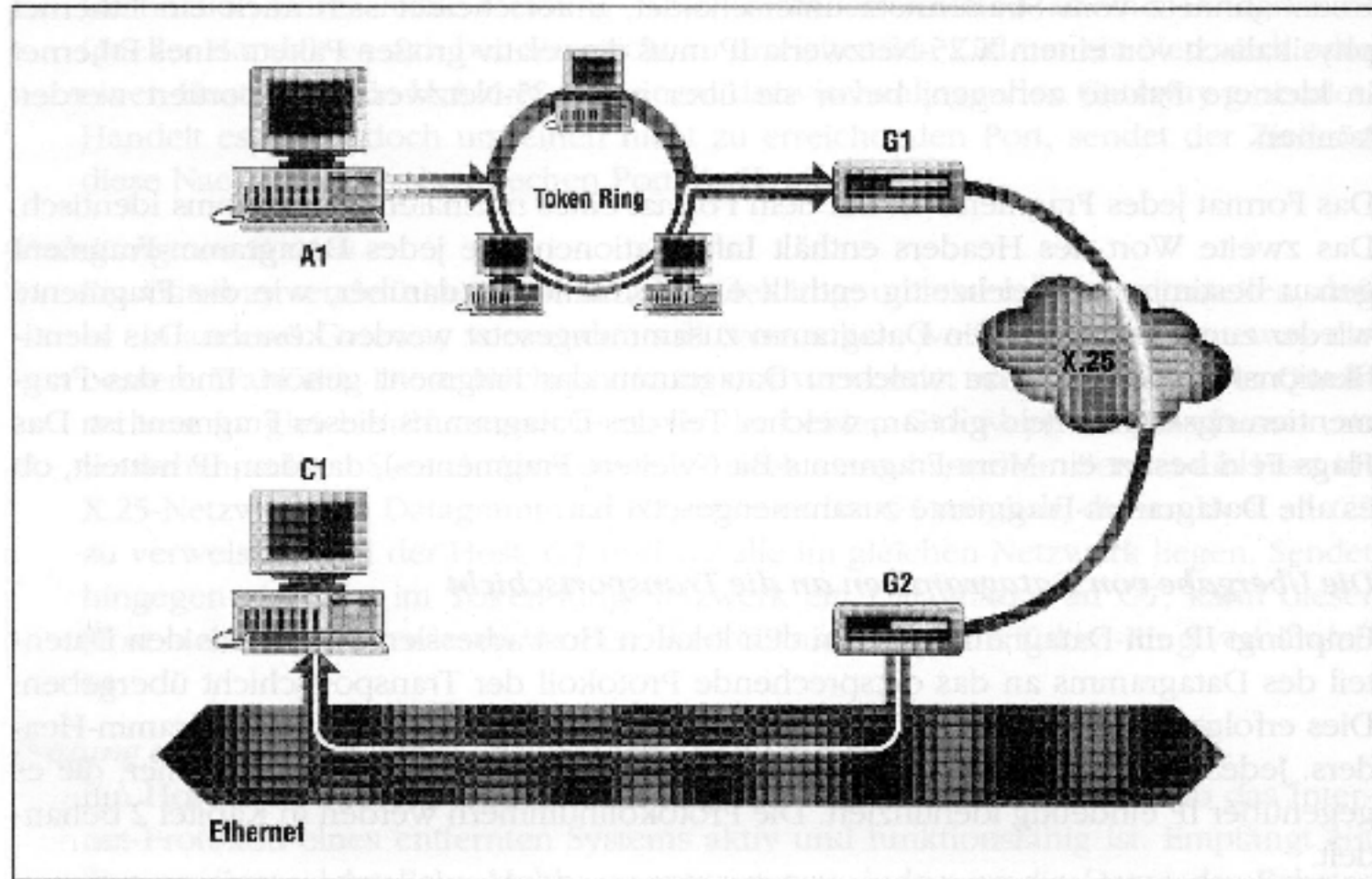


Abbildung 1-7: Netzwerke, Gateways und Hosts



Host-zu-Host-Transportschicht

- **UDP:** User Datagram Protocol:
Verbindungsloser Dienst ohne Flusskontrolle, aber in bestimmten Fällen besser verwendbar als TCP (VoIP, Tracking, ...).
- **TCP:** Transmission Control Protocol:
 - Verbindungsorientierter, sicherer Transportdienst durch positive Rückmeldungen und ggf. Data-gramm-Wiederholung („Bytestream“).
 - TCP ist voll-duplex-fähig, benutzt ein „Sliding-Window-Verfahren“ und kennt Vorrang-Daten.



Aufbau des UDP-Headers

- Ports (16 Bit): Quell- und Zielport
- Länge (16 Bit) des Paketes
- Checksum (16 Bit) des Paketes (optional)
- Es folgen die Daten.
- UDP ist sehr schlank und effizient, wenn es nicht auf einen kontinuierlichen und garantiert sequentiellen Datenfluss ankommt.

Aufbau des TCP-Headers

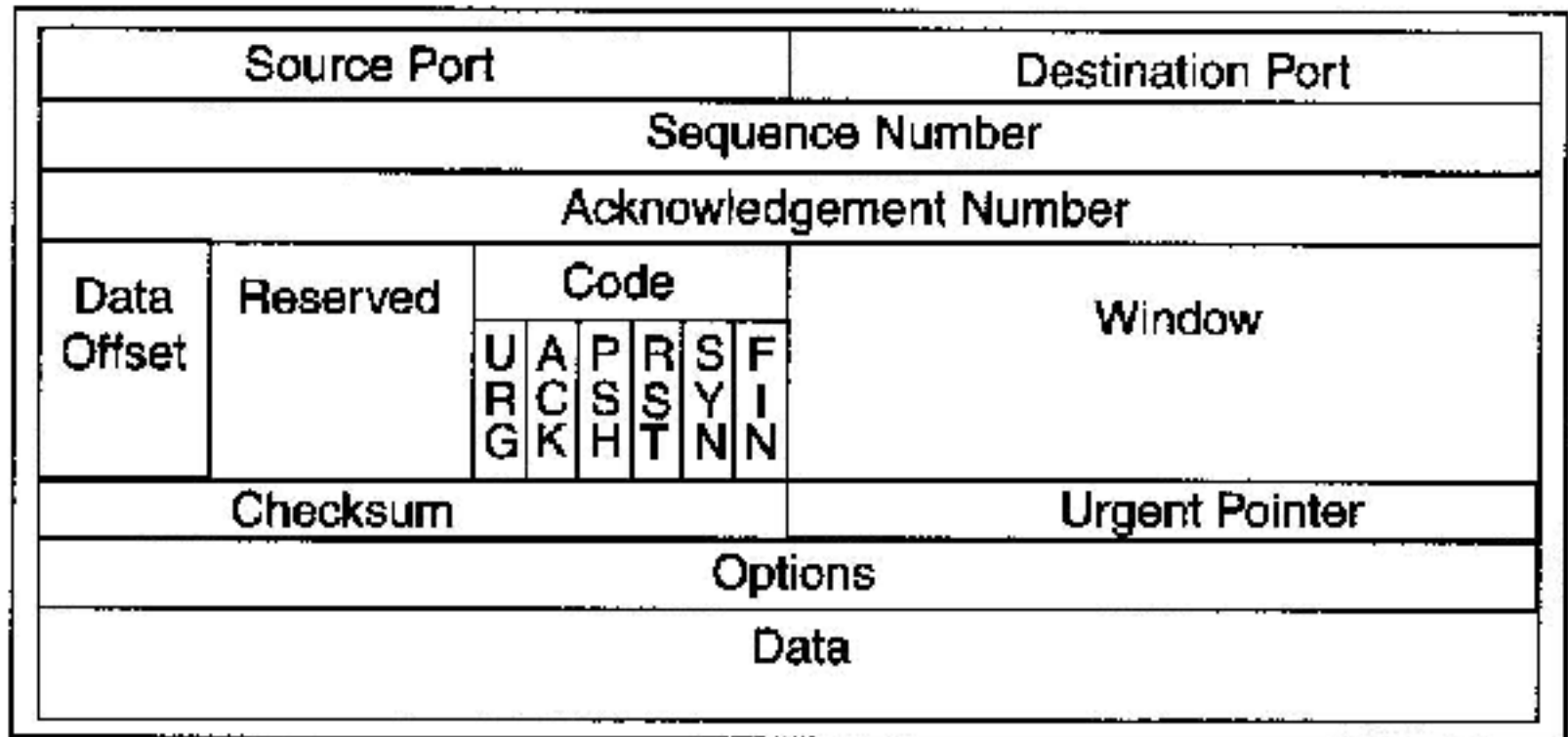


Abbildung 9.14: Aufbau eines TCP-Blocks



Wichtige Felder TCP-Header (1)

- **Source/Destination Port:** Sende- und Empfangsports = „Anwendungen“
- **Sequence Number:** Pointer auf die Position der Daten im Datenstrom
- **Acknowledgement-Number:** Bestätigt einen Teil des Stroms positiv (-> Seq. Number)
- **Data Offset:** Wo fangen die Daten an?
- **Window:** Anzahl Bytes, die ohne ACK gesendet werden dürfen (dynamisch)



Wichtige Felder TCP-Header (2)

- Code:
 - URG: Urgent Pointer beachten
 - ACK: Positive Quittung enthalten
 - PSH: „Push“, sofortiges Weiterleiten ohne Pufferung erwünscht.
 - RST: Reset, Verbindung abbauen.
 - SYN: Synchronisierung auf Sequence Number.
 - FIN: Graceful shutdown der Verbindung.
- Checksum: 16-Bit-Längsparität über alles.
- Urgent Pointer: Diese Daten durchreichen!

TCP-Stream

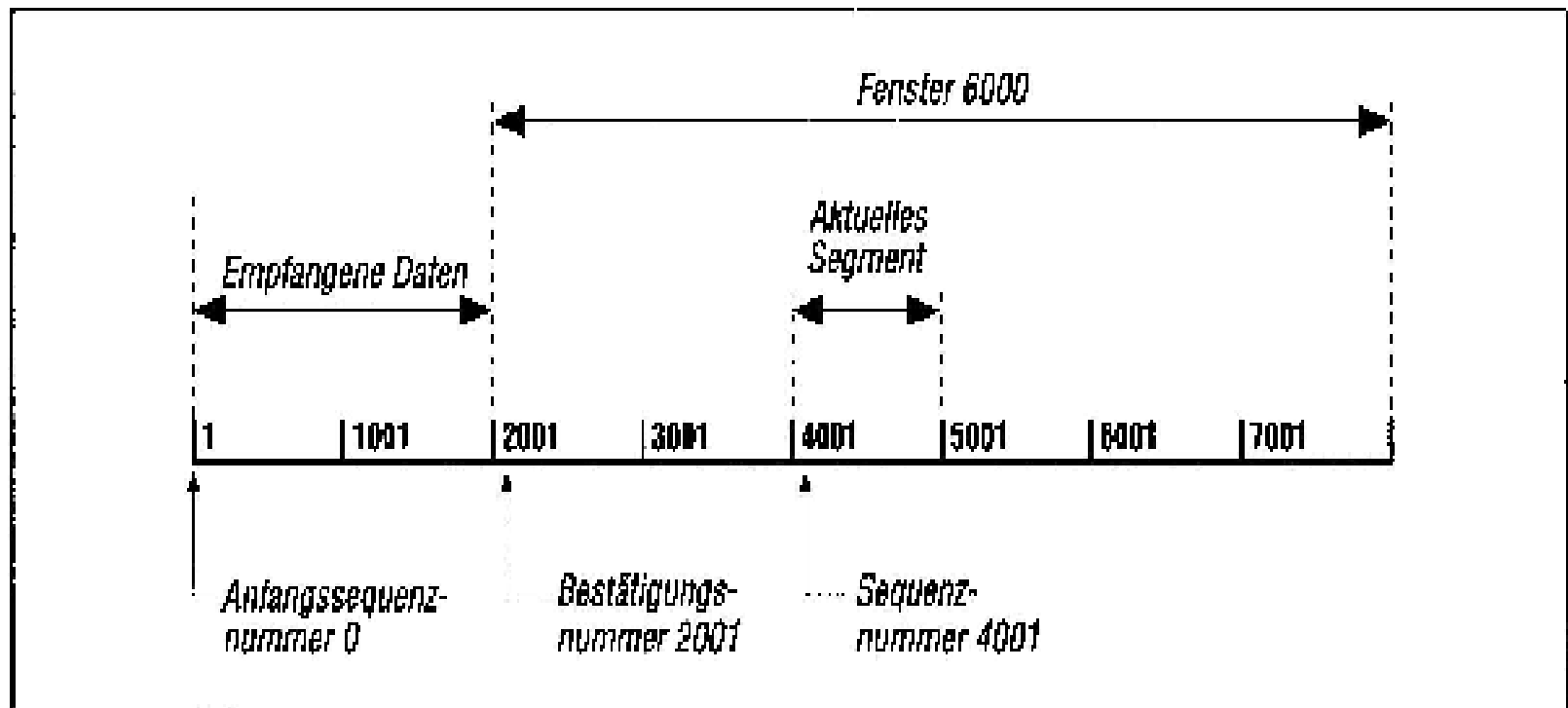


Abbildung 1-11: Ein TCP-Stream

Ablauf TCP-Protokoll

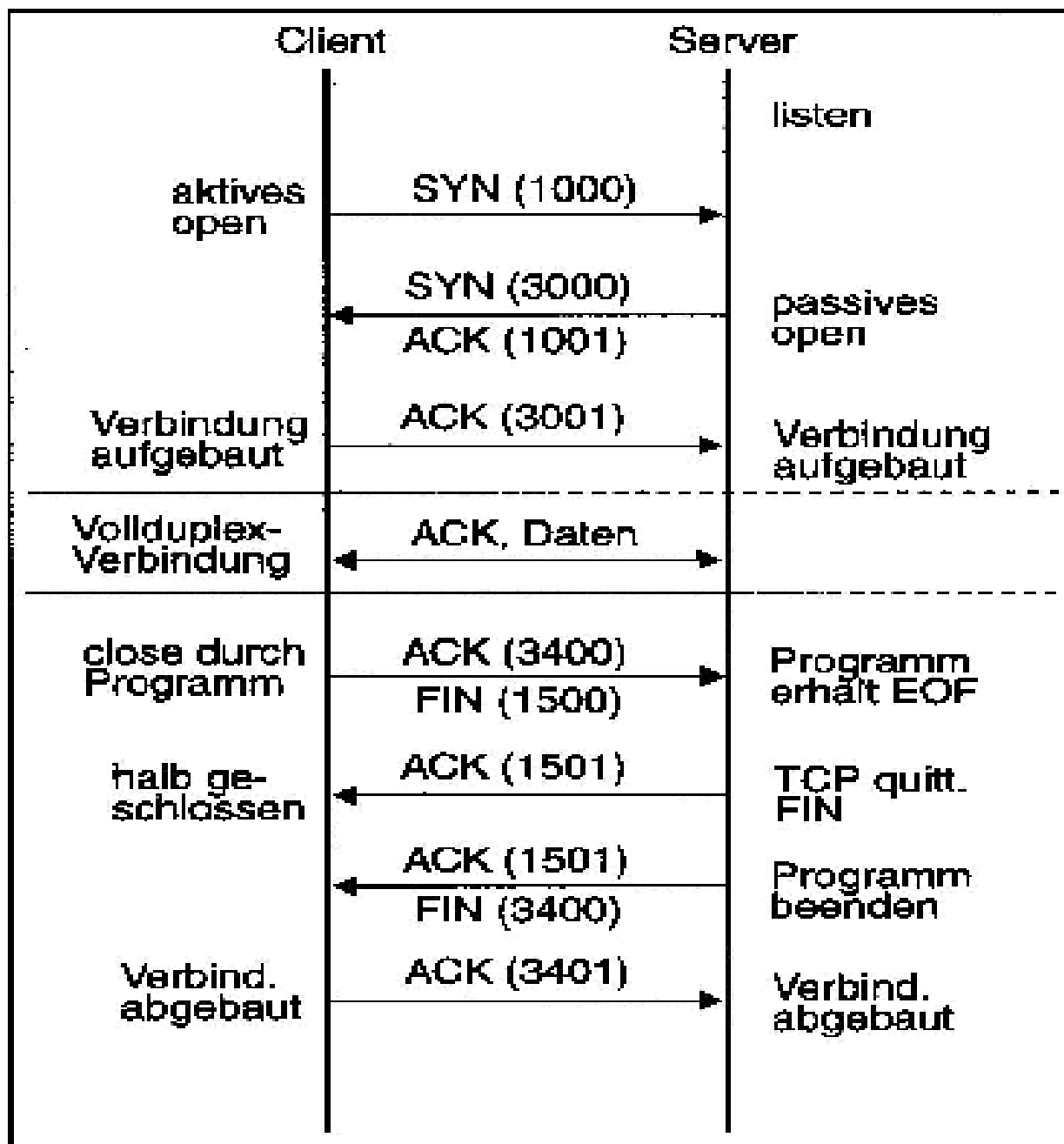


Abbildung 9.15: Ablauf einer TCP-Session



Verbindungs-Zustände TCP

- LISTEN: Warten auf Connection Request
- SYN-SENT: SYN gesendet, Warten auf ACK
- SYN-RECEIVED: ACK/SYN gesehen, ACK gesendet, warten auf erste Daten
- ESTABLISHED: ACK/Daten gesehen, full duplex
- FIN-WAIT-1: FIN gesendet, warten auf ACK.
- FIN-WAIT-2: ACK gesehen, warten auf FIN.
- CLOSE-WAIT: Warten auf CLOSE der darüber liegenden Anwendung
- CLOSING: Warten auf ACK/FIN
- LAST-ACK: Warten auf ACK zum letzten FIN.



Anwendungs-Schicht

- Wohl bekannt: telnet, ftp, smtp, http.
- Ausserdem: dns, nfs, samba, ldap, ...
- Und: rlogin, rcp, ssh, scp, sftp, ...
- Datenbanken: odbc, jdbc, nativer Zugang.
- ...



Linux-Tools fürs Netzwerk

- ifconfig, route: Konfiguration des Interfaces.
- netstat: Verbindungen und Zustände.
- ping, traceroute: Netzwerk durchstöbern.
- hostname, unname, dig, nslookup, whois: Namen, Netze, Auflösung, Eigentümer.
- arp, rarp: Hardware-Adressen <-> IP-Adr.
- tcpdump: Das Swiss Army Knife des Admin
- iptraf: Einfachere Variante, „alte“ Oberfläche



Aufgabe für die Übung

- Informieren Sie sich über die genannten Tools mittels des man Befehls.
- Suchen Sie Anleitungen und Dokumentationen im Internet.
- Beispiel: www.tcpcat.com

Versuch macht kluch, pflegte Tony Curtis in „Die Zwei“ zu Roger Moore zu sagen.